PEMBUATAN APLIKASI DETEKSI INTRUSI MULTI ENGINE

Prima Wiratama[1], Idris Winarno S.kom M.kom[2],Isbat uzzin Nadhori S.kom[3]
[1]Mahasiswa Jurusan Teknik Informatika, [2]Dosen Jurusan Teknik Informatika
[3]Dosen JurusanTeknik Informatika
Jurusan Teknik Informatika
Politeknik Elektronika Negeri Surabaya
Institut Teknologi Sepuluh Nopember Surabaya
Kampus ITS Sukolilo, Surabaya 60111, Indonesia
Tel: +62 (31) 594 7280; Fax: +62 (31) 594 6114
e-mail : panberprime@yahoo.co.id Idris_nano@yahoo.com isbat@eepis.its.edu

Abstrak

Pada masa kini, terdapat banyak peningkatan yang signifikan terhadap pengembangan dari sistem teknologi deteksi intrusi. Namun, pada saat yang sama pula, teknologi dari intrusi juga semakin meningkat dan canggih. Sebagai contoh adalah lebih dari 359.000 komputer diperkirakan telah terinfeksi *worm* jenis *Code-Red* hanya dalam hitungan 14 jam pada tahun 2001, dengan kerugian mencapai lebih dari $2 miliyar.Masalah-masalah yang timbul dalam menjaga suatu jaringan diantaranya adalah: Pertama, metode dan teknologi yang digunakan oleh penyerang terus berkembang. Kedua adalah kelemahan yang dimiliki pada suatu software dan kompleksitas dari internet membuat sistem deteksi sulit melakuan perlindungan terhadap sistem. Ketiga, arsitektur dari sistem deteksi intrusi yang terpusat membuat sistem mudah untuk dirusak seperti menggunakan pola serangan *denial of service*. Dari permasalahan-permasalah yang ada tersebut maka timbulah suatu metode untuk menanggulanginya yaitu dengan menggunakan metode kolaborasi sistem deteksi intrusi. Kolaborasi antar sistem deteksi intrusi dapat mendeteksi intrusi secara cepat dan akurat karena sistem melakukan pertukaran informasi tentang sumber-sumber yang mencurigakan.

Kata Kunci: *IDS,multi engine*

1. PENDAHULUAN

1.1 LATAR BELAKANG

Seiring dengan perkembangan teknologi maka ilmu semakin lama juga akan semakin berkembang. Seiring dengan berkembangnya ilmu, teknologi juga bertanbah canggih hal ini diikuti dengan bertambah canggihnya kejahatan dalam dunia *Cyber* dengan banyaknya usaha *cracking* terhadap sistem jaringan komputer Oleh pihak-pihak yang tidak berhak.

Dengan adanya permasalahan seperti diatas.maka semakin bermunculan juga aplikasi-aplikasi untuk keamanan jaringan. Salah satu diantaranya adalah IDS *(Intrusion Detection System)* definisi dari IDS ini adalah *Software* atau *Hardware* yang dapat mendeteksi dan melakukan *logging* terhadap aktifitas yang tidak diinginkan atau aktifitas yang aneh.Dengan cara ini IDS dapat melindungi dari kehilangan data atau intrusi.

1.2 PERUMUSAN MASALAH

Prosedur / tahapan pembangunan sistem adalah sebagai berikut:

- Pembacaan file log IDS
  Pembacaan file log IDS diperlukan untuk menerima masukan data berupa IP penyerang, nomor IP yang diserang, nomor port yang diserang, dan jenis serangan yang dilakukan berdasarkan report yang dihasilkan IDS melalui *file log IDS* tersebut yang berupa *file* teks secara terus-menerus.
- Pemblokiran Penyerang
  Pemblokiran penyerang sangat diperlukan untuk mencegah intrusi dari penyerang tersebut.Pemblokiran penyerang dapat dilakukan dengan melakukan kolaborasi dengan firewall yang terpasang di sistem operasi yang digunakan.pemblokiran dilakukan berdasarkan data-data yang dihasilkan dari proses *parsing file log IDS*.
- Broadcasting data dengan socket
  Transfer data perlu dilakukan untuk mencegah penyerang memasuki komputer lain dalam jaringan agar dapat melakukan pemblokiran penyerang tersebut. *Broadcasting* dapat dilakukan dengan *socket* yang dibuat dengan program java. Penggunaan java socket ini dikarenakan sifat dari bahasa pemrograman java yang *multi platform*.

1.3 BATASAN MASALAH

Aplikasi yang akan digunakan ada 3 engine IDS:

1. snort
2. psad
3. portsentry

1.4 TUJUAN

Tujuan proyek akhir ini adalah untuk membuat suatu jaringan menjadi lebih aman dengan adanya IDS *multi engine*. hal ini dikarenakan adanya aplikasi yang berguna untuk melakukan *broadcasting alert* ke semua *client*.sehingga ini akan sangat membantu apabila *signature* salah satu engine IDS belum diperbaharui.

2. PERANCANGAN SISTEM

2.1 RANCANGAN UMUM

pada dasarnya proyek akhir ini adalah membuat suatu aplikasi yang dapat digunakan untuk menggabungkan kerja beberapa IDS yang terkoneksi dan terinstal di komputer-komputer jaringan dalam mendeteksi sebuah serangan.dengan cara melakukan parsing file log IDS tersebut kemudian alert yang didapat diteruskan ke komputer lain dalam jaringan untuk kemudian dilakukan pemblokiran IP penyerang.

2.1.1.Perancangan Data

a) Kebutuhan Input

Kebutuhan input sistem digolongkan menjadi 2, yaitu antara lain :

Data Input

Data-data input yang dibutuhkan adalah :

- software IDS(snort,portsentry,PSAD)
- File Log IDS
- IP penyerang ,IP yang diserang,dan alert. Ip address server

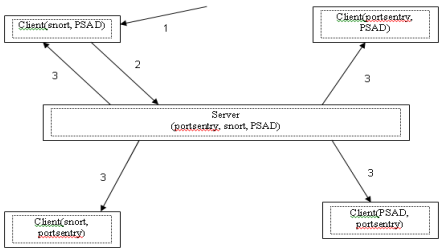
b) Kebutuhan Output

Hasil akhir dari sistem ini adalah berupa data tentang intrusi yang terjadi pada seluruh komputer pada jaringan.

2.2 Perancangan Sistem

2.2.1. Diagram Sistem

Untuk perancangan antarmuka, di bawah ini akan ditunjukkan blok arsitektur sistem yang digunakan pada sistem ini :



Gambar 2.2.1 Diagram Sistem

2.2.2. Diagram Alir (Flowchart) Sistem

Secara umum, sistem yang akan dibangun dapat digambarkan (server dan client) dalam bentuk diagram alir (flowchart) berikut ini :

- Pembacaan file log IDS

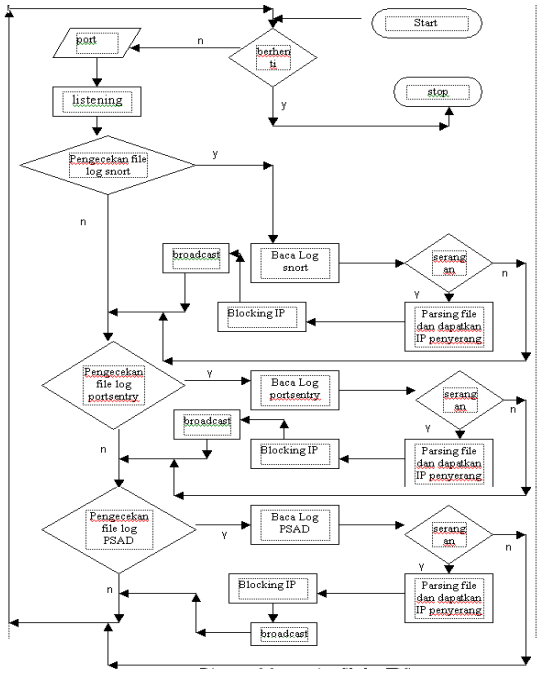


Diagram 2.2.2.1 Diagram Alir (*Flowchart*) Pembacaan file log IDS

- Pemblokiran penyerang

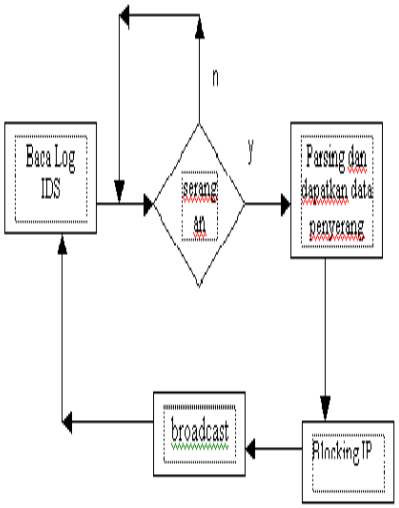


Diagram 2.2.2.2 Diagram Alir (*Flowchart*) Pemblokiran penyerang

- Broadcasting alert dengan socket

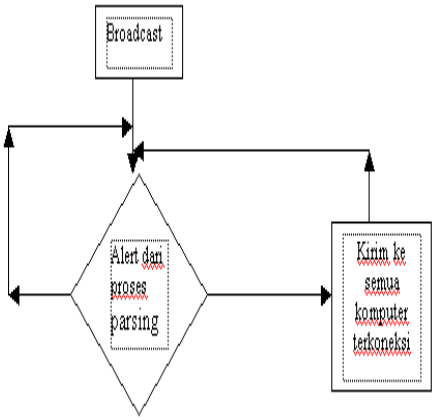


Diagram 2.2.2.3 Diagram Alir (*Flowchart*) Broadcasting alert dengan socket

- Pembacaan log IDS dilakukan untuk membaca file hasil loging dari snort, PSAD dan portsentry. File hasil loging atau disebut juga alert akan berisi sebuah informasi penyerangan yang dilakukan oleh penyusup dalam jaringan. Informasi yang bisa diperoleh dari alert ini adalah ip penyerang ,jenis serangan, ,IP dan port yang diserang dan juga destination IP (host target) Alert dari snort dan portsentry masing-masing secara default terletak pada direktori /var/log/snort/alert,/var/log/psad/status.out dan /var/log/messages. Proses pembacaan log dari IDS ini adalah sebagai berikut:
- Melakukan pembacaan terhadap string alamat direktori dari snort ,PSAD dan portsentry. Setelah diketahui bahwa pada alamat tersebut terdapat file maka akan dilakukan looping untuk membaca subalert yang terdapat dalam file tersebut dengan cara membaca kata perkata pada file log.
- Hasil pembacaan subalert IDS tersebut akan disimpan dalam suatu List. Subalert adalah bagian dari alert seperti ip penyerang,ip korban,jenis serangan dan port yang diserang, jadi ada 4 subalert yang digunakan dan subalert-subalert ini akan di simpan pada list yang berbeda-beda.
- Subalert-subalert akan disatukan di program server-side dan untuk di sebarkan ke client atau dikirimkan ke server dan program client-side juga akan melakukan penyatuan subalert-subalert untuk kemudian dikirimkan ke server.
- Pemblokiran penyerang sangat penting dilakukan untuk mencegah penyerang melakukan penyusupan ke system dalam jaringan.program akan menerima string yang didapat dari isi list subalert ip penyerang kemudian akan memanggil iptables untuk melakukan pemblokiran terhadap ip penyerang tersebut.
- Broadcasting berguna untuk mengirimkan subalert yang telah disatukan dengan subalert lainya ke semua client program diatas dapat menghandle 65534 client apabila client terkoneksi maka program akan membuat thread baru tiap thread akan menghandle 1 client program akan memeriksa thread apakah alert sudah dikirim ke client apabila belum alert akan dikirim ke client tersebut jika sudah,alert tidak dikirim ke client tersebut. Sampai semua client yang terhubung mendapat alert.

3. Implementasi Sistem

3.1. Perangkat Lunak Pendukung

Perangkat lunak yang digunakan dalam pembangunan sistem ini adalah antara lain :

a) Linux versi 2.4
b) Java SE Development Kit (JDK) 6 Update 14.
c) NetBeans 5.0.
d) iptables aktif
e) salah satu atau beberapa dari IDS berikut(snort,portsentry,PSAD).

3.2. Persiapan Sistem

Agar sistem dapat dijalankan perlu dilakukan dilakukan konfigurasi sebagai berikut:
Install salah satu atau beberapa IDS dengan cara mengetikan perintah:
 # yum install <nama-program>
untuk pengguna yang menginstall PSAD dilakukan konfigurasi tambahan:
 # nano /etc/syslog.conf
akan ditampilkan isi file syslog.conf
 # kern. /dev/console*
edit baris diatas menjadi:
kern. /var/log/firewall.log*
simpan perubahan dan restart service syslog
#service syslog restart
edit file /etc/psad/psad.conf
#nano /etc/psad/psad.conf
edit baris berikut:
ENABLE_AUTO_IDS N;
IPT_SYSLOG_FILE /var/log/messages;
Menjadi:
ENABLE_AUTO_IDS Y;
IPT_SYSLOG_FILE /var/log/firewall.log;
Simpan dan restart service PSAD
#service psad restart
hapus semua rule iptables dan buat rule untuk logging
#iptables –F
#iptables –I INPUT 1 –i eth0 –j LOG –log-level 7
#iptables –I FORWARD 1 –i eth0 –j LOG –log-level 7

3.3. Perancangan Sistem

Dari desain sistem yang telah kita buat sebelumnya, maka dapat kita implementasikan seperti berikut :

- Pembacaan log IDS dilakukan untuk membaca file hasil loging dari snort, PSAD dan portsentry. File hasil loging atau disebut juga alert akan berisi sebuah informasi penyerangan yang dilakukan oleh penyusup dalam jaringan. Informasi yang bisa diperoleh dari alert ini adalah ip penyerang ,jenis serangan, ,IP dan port yang diserang dan juga destination IP (host target) Alert dari snort dan portsentry masing-masing secara default terletak pada direktori /var/log/snort/alert,/var/log/psad/status.out dan /var/log/messages. Proses pembacaan log dari IDS ini adalah sebagai berikut:
- Melakukan pembacaan terhadap string alamat direktori dari snort ,PSAD dan portsentry. Setelah diketahui bahwa pada alamat tersebut terdapat file maka akan dilakukan looping untuk membaca subalert yang terdapat dalam file tersebut dengan cara membaca kata perkata pada file log.
- Hasil pembacaan subalert IDS tersebut akan disimpan dalam suatu List. Subalert adalah bagian dari alert seperti ip penyerang,ip korban,jenis serangan dan port yang diserang, jadi ada 4 subalert yang digunakan dan subalert-subalert ini akan di simpan pada list yang berbeda-beda.
- Subalert-subalert akan disatukan di program server-side dan untuk di sebarkan ke client atau dikirimkan ke server dan program client-side juga akan melakukan penyatuan subalert-subalert untuk kemudian dikirimkan ke server.
- Pemblokiran penyerang sangat penting dilakukan untuk mencegah penyerang melakukan penyusupan ke system dalam jaringan.program akan menerima string yang didapat dari isi list subalert ip penyerang kemudian akan memanggil iptables untuk melakukan pemblokiran terhadap ip penyerang tersebut.
- Broadcasting berguna untuk mengirimkan subalert yang telah disatukan dengan subalert lainya ke semua client program diatas dapat menghandle 65534 client apabila client terkoneksi maka program akan membuat thread baru tiap thread akan menghandle 1 client program akan memeriksa thread apakah alert sudah dikirim ke client apabila belum alert akan dikirim ke client tersebut jika sudah,alert tidak dikirim ke client tersebut. Sampai semua client yang terhubung mendapat alert.

4. Kesimpulan

Berdasarkan analisa dari beberapa pengujian pada bab sebelumnya, kesimpulan yang didapatkan adalah :

Sistem dapat menghasilkan report report yang dapat digunakan untuk identifikasi serangan IDS. Dan melakukan pemblokiran dan melakukan broadcasting alert.

5. Daftar Pustaka

- Liang, Daniel. "*Comperhensive version introduction to Java Programming Seventh edition*"New jersey,: Upper saddle River, 2005.
- Mohammad, hendy alva."Rahasia dan trik mengamankan Server Linux". Surabaya: 2006.
- Purnama, Rangsang, "*Tutunan Pemrogramman Java jillid 1* ", Prestasi pustaka publisher,surabaya 2005.
- Sto, "*wireless Kung fu Networking& hacking*", Jakarta: 2007.
- http://id.wikipedia.org/wiki/SYN_flooding_attack SYN flooding attack 14/03/2010
- http://id.wikipedia.org/wiki/Nmap nmap 14/03/2010